

ON THE ESSENTIAL DIMENSION OF UNIPOTENT ALGEBRAIC GROUPS

NGUYỄN DUY TÂN

ABSTRACT. We give an upper bound for the essential dimension of a smooth unipotent algebraic group over an arbitrary field. We also show that over a field k which is finitely generated over a perfect field, a smooth unipotent algebraic k -group is of essential dimension 0 if and only if it is k -split.

AMS Mathematics Subject Classification (2010): 11E72 (20D15).

1. INTRODUCTION

Let k be a base field, \mathbf{Fields}_k the category of field extensions K/k , \mathbf{Sets} the category of sets. Let $\mathcal{F} : \mathbf{Fields}_k \rightarrow \mathbf{Sets}$ be a covariant functor. Given a field extension K/k , we will say that $a \in \mathcal{F}(K)$ *descends* to an intermediate field $k \subset K_0 \subset K$ if a is in the image of the induced map $F(K_0) \rightarrow F(K)$. The *essential dimension* $\mathrm{ed}_k(a)$ of $a \in \mathcal{F}(K)$ is the minimum of the transcendence degrees $\mathrm{trdeg}_k(K_0)$ taken over all fields $k \subset K_0 \subset K$ such that a descends to K_0 . The essential dimension $\mathrm{ed}_k(\mathcal{F})$ of the functor \mathcal{F} is the supremum of $\mathrm{ed}(a)$ taken over all $a \in \mathcal{F}(K)$ with K in \mathbf{Fields}_k .

If G is an algebraic group over k , we write $\mathrm{ed}_k(G)$ for the essential dimension of the functor $K \mapsto H_{\mathrm{fppf}}^1(K, G)$. The notion of essential dimension of a finite group is introduced by Buhler and Reichstein ([BR]). The definition of the essential dimension of a functor is a generalization given later by Merkujev ([BF]). In [BRV1], the authors introduce a notion of essential dimension for algebraic stack, see also [BRV2]. Nowadays, studying essential dimension is an active area. See [Re] and reference therein.

Computing the essential dimension of algebraic groups is, in general, a hard problem. By the work of [Fl, KM], one now can compute the essential dimension of finite (abstract) p -groups over a field of characteristic different from p . In [LMMR], the authors study also the essential dimension of algebraic tori. However, we do not know much about the essential dimension of finite p -groups over a field of characteristic $p > 0$ in particular, and the essential dimension of unipotent algebraic groups in general. Let k be a field of characteristic $p > 0$ and G be a finite p -group of order p^n . Then, Ledet [Le] shows that $\mathrm{ed}_k(G) \leq n$. He also conjectures that $\mathrm{ed}_k(\mathbb{Z}/p^n\mathbb{Z}) = n$. As noted by Reichstein [Re, Subsection 7.3]: This seems to be out of reach at the moment, at least for $n \geq 5$. Tossici and Vistoli [TV] shows also that the above inequality, $\mathrm{ed}_k(G) \leq n$, still holds for any finite (not necessarily smooth) trigonalizable k -group scheme G of order p^n , where $p = \mathrm{char} k$.

Partially supported by the NAFOSTED, the SFB/TR45 and the ERC/Advanced Grant 226257.

In this paper, we study the essential dimension of a unipotent algebraic group over a field. An *algebraic group* over a field k is a k -group scheme of finite type over k . The smooth affine algebraic k -groups considered here are the same as linear algebraic groups defined over k in the sense of [Bo]. Recall that an affine algebraic k -group G is called *unipotent* if $G_{\bar{k}}$ (the base change of G to a fixed algebraic closure \bar{k} of k) admits a finite composition series over \bar{k} with each successive quotient isomorphic to a \bar{k} -subgroup of the additive group \mathbb{G}_a . It is well-known that an affine algebraic k -group G is unipotent if and only if it is k -isomorphic to a closed k -subgroup scheme of the group T_n consisting of upper triangular matrices of order n with all 1 on the diagonals, for some n .

A smooth unipotent algebraic group G over a field k is called *k -split* if it admits a composition series by k -subgroups with successive quotients are k -isomorphic to the additive group \mathbb{G}_a . We say that G is *k -wound* if every map of k -scheme $\mathbb{A}_k^1 \rightarrow G$ is a constant map to a point in $G(k)$.

For any smooth unipotent algebraic group G defined over k , there is a maximal k -split k -subgroup G_s , and it enjoys the following properties: it is normal in G , the quotient G/G_s is k -wound and the formation of G_s commutes with separable (not necessarily algebraic) extensions, see [Oe, Chapter V, 7] and [CGP, Theorem B.3.4]. The group G_s is called the *k -split part* of G . We obtain the following result.

Theorem 1.1. *Let G be a smooth unipotent algebraic group over a field k , G_s its k -split part and let H be the quotient G/G_s . Let H^0 be the identity component of H . Let p^n be the order of H/H^0 if $p = \text{char}(k) > 0$ and let $n = 0$ if $\text{char}(k) = 0$. Then*

$$\text{ed}_k(G) \leq \text{ed}_k(H/H_0) + \dim(G/G_s) \leq n + \dim(G/G_s).$$

In Section 2, we prove a technical result, Proposition 2.2, which is needed in proving Theorem 1.1. In [TV, Lemma 3.4], the authors prove the proposition for (not necessarily smooth) affine group schemes but under the assumption that A is a *commutative* unipotent normal subgroup scheme of B (notations as in Proposition 2.2). In fact, they need the commutativity property of A in their proof. Since all groups considered in Proposition 2.2 are supposed to be smooth, we can use the language of cocycles and non-abelian cohomology theory as developed in [Se2] and we can relax the commutativity condition on A .

In Section 3, we give some results concerning the essential dimension of finite étale group schemes of p -power order over fields of characteristic $p > 0$. Some of the results are already appeared in [JLY] in the case of finite abstract p -groups.

In this Section 4, we first give an upper bound for the essential dimension of smooth connected unipotent algebraic groups and then by combining with a result in Section 3, we prove Theorem 1.1.

In the last section, we study smooth unipotent algebraic groups of essential dimension 0. Let G be an smooth affine algebraic group over a field k . It can be shown that $\text{ed}_k(G) = 0$ if and only if G is *special*, i.e., for any field extension L/k , every G -torsor over $\text{Spec } L$ is trivial, see [Me, Proposition 4.4] and [TV, Proposition 4.3]. Special groups are introduced by Serre in [Se1]. Over algebraic closed fields, they are classified by Grothendieck [Gro].

Studying smooth unipotent algebraic groups of essential dimension 0 is therefore equivalent to studying smooth unipotent algebraic groups which are special. It is well-known that over a perfect field k , every smooth connected unipotent group G is k -split (see e.g. [Bo, Chapter V, Corollary 15.5 (ii)]), and hence special. Therefore, over a perfect field, a smooth unipotent group is special if and only if it is k -split. (Note that a special algebraic group is always connected [Se1].) It turns out that this statement still holds true over certain fields, e.g., fields which are finitely generated over a perfect field. Namely, we have

Theorem 1.2. *Let k_0 be a field of characteristic $p > 0$, v a valuation of k_0 . We assume that there is a k_0^p -basis $\{e_1, \dots, e_n\}$ of k_0 such that $v(e_1), \dots, v(e_n)$ are pairwise distinct modulo p . Let k be a finite extension of k_0 . Let G be a non-trivial smooth unipotent algebraic k -group. Then G is special if and only if G is k -split.*

This theorem yields the following corollary (see Corollary 6.10 for a more general statement).

Corollary 1.3. *Let k be a field which is finitely generated over a perfect field. Let G be a non-trivial smooth unipotent algebraic k -group. Then $\text{ed}_k(G) = 0$ if and only if G is k -split.*

To prove Theorem 1.2 and Corollary 1.3, we need some results concerning the images of additive maps over valued fields. These results are presented in Section 5.

We do not know whether Theorem 1.2 is still true over an *arbitrary* field k .

Question 1.4. Let k be a field, G a smooth unipotent algebraic k -group. Is this true that $\text{ed}_k(G) = 0$ if and only if G is k -split? Equivalently, is this true that G is special if and only if k -split?

Acknowledgements: We would like to give our sincere thanks to H  l  ne Esnault for her support and constant encouragement. We would like to thank Nguyễn Quốc Th  ng for his interest in the paper.

2. A TECHNICAL RESULT

For a smooth algebraic group over a field k , the flat cohomology $H_{\text{fppf}}^1(K, G)$ is the same as the Galois cohomology $H^1(K, G)$ for any field extension K/k . We need the following lemma.

Lemma 2.1. *Let k be a field. G a smooth affine algebraic k -group. Let U be a normal unipotent k -subgroup of G . Then the natural map*

$$\varphi : H^1(k, G) \rightarrow H^1(k, U)$$

is surjective.

Furthermore, if in addition that U is k -split then φ is a functorial bijection.

Proof. See [Oe, Chapter IV, 2.2, Remark 3] for the first statement.

See [GM, Lemma 7.3] for the second statement. □

We have following key technical result, which is motivated by [TV, Lemma 3.4].

Proposition 2.2. *Let k be a field and consider an exact sequence of smooth affine algebraic k -groups*

$$1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1,$$

where A is a unipotent normal subgroup of B . Let K/k be a field extension and x an element in $H^1(K, B)$. Then there exists a subfield extension $k \subset E \subset K$ and a twisted form \tilde{A} of $A_E = A \times_k E$, \tilde{A} is defined over E , such that

$$\text{ed}(x) \leq \text{ed}_k(C) + \text{ed}_E(\tilde{A}).$$

Further, if A is central in B then one can choose $\tilde{A} = A_E$ and in particular

$$\text{ed}_k(B) \leq \text{ed}_k(C) + \text{ed}_k(A).$$

Proof. Denote by $g_- : H^1(-, B) \rightarrow H^1(-, C)$ the natural morphism of functors induced from $B \rightarrow C$. Set $y = g_K(x) \in H^1(K, C)$, then there exists a subfield extension $k \subset E \subset K$ and z in $H^1(E, C)$ such that $\text{trdeg}(E : k) = \text{ed}(y) \leq \text{ed}_k(C)$ and the image of z via $H^1(E, C) \rightarrow H^1(K, C)$ is equal to y . Since the natural map $g_E : H^1(E, B) \rightarrow H^1(E, C)$ is surjective, there exists t in $H^1(E, B)$ such that $g_E(t) = z$. Let b be a cocycle in $Z^1(E, B)$ representing t and let c be the image of b in $Z^1(E, C)$. Denote by ${}_bA$, ${}_bB$ and ${}_cC$ the groups obtaining by twisting A , B and C (more precisely, by twisting A_E , B_E and C_E) using the cocycles b , b and c respectively. Then we get the following exact sequence of E -groups

$$1 \rightarrow {}_bA \rightarrow {}_bB \rightarrow {}_cC \rightarrow 1$$

by twisting the initial sequence.

Recall that there is a functorial bijection between $H^1(L, {}_bH)$ and $H^1(L, {}_bH)$ for any k -group H , 1-cocycle $b : \text{Gal}(k_s/k) \rightarrow H(k_s)$, and field extension L/k (see [Se2, I, 5.3, Proposition 35]). Thus in the following commutative diagram, the maps p, q, p', q' are all bijective

$$\begin{array}{ccccc}
 & & H^1(E, B) & \xrightarrow{g_E} & H^1(E, C) \\
 & \nearrow p & \downarrow \beta & & \searrow q \\
 H^1(E, {}_bB) & \xrightarrow{g'_E} & H^1(E, {}_cC) & & \\
 \downarrow \beta' & & \downarrow \gamma' & & \downarrow \gamma \\
 & \nearrow p' & H^1(K, B) & \xrightarrow{g_K} & H^1(K, C) \\
 H^1(K, {}_bA) & \xrightarrow{f'_K} & H^1(K, {}_bB) & \xrightarrow{g'_K} & H^1(K, {}_cC)
 \end{array}$$

Note that the bottom row in the above diagram is an exact sequence of pointed sets.

Since we twist by the cocycle representing t , we have $t = p(1)$, where by abuse of notation, 1 denote the trivial cohomology class. Since p' is bijective, there exists $x' \in H^1(K, {}_bB)$ such that $x = p'(x')$. We have

$$\begin{aligned}
 y &= g_K(x) = g_K \circ p'(x') = q' \circ g'_K(x') \\
 &= \gamma(z) = \gamma(g_E(t)) = \gamma \circ g_E \circ p(1) = q' \circ g'_K \circ \beta'(1) = q'(1).
 \end{aligned}$$

Since q' is bijective, $g'_K(x') = 1$. Hence there exists $u' \in H^1(K, {}_bA)$ such that $x' = f'_K(u')$. By definition of $\text{ed}_E(u')$, there is a subfield extension $E \subset E' \subset K$ and an element $v' \in H^1(E', {}_bA)$ such that $\text{trdeg}(E' : E) \leq \text{ed}_E({}_bA)$ and u' is the image of v' via $H^1(E', {}_bA) \rightarrow H^1(K, {}_bA)$. (Note that ${}_bA$ is only defined over E .) From the following commutative diagram

$$\begin{array}{ccccc}
 & & & & H^1(K, B) , \\
 & & & \nearrow p' & \uparrow \beta_1 \\
 H^1(K, {}_bA) & \xrightarrow{f'_K} & H^1(K, {}_bB) & & \\
 \uparrow \alpha'_1 & & \uparrow \beta'_1 & & \\
 H^1(E', {}_bA) & \xrightarrow{f'_{E'}} & H^1(E', {}_cB) & \nearrow p'_1 & H^1(E', B)
 \end{array}$$

we get

$$x = p'(x') = p' \circ f'_K(u') = p' \circ f'_K \circ \alpha'_1(v') = \beta_1 \circ p'_1 \circ f'_{E'}(v').$$

Therefore, $x \in \text{im}(\beta_1)$ and hence

$$\text{ed}(x) \leq \text{trdeg}(E' : k) = \text{trdeg}(E' : E) + \text{trdeg}(E : k) \leq \text{ed}_k(C) + \text{ed}_E({}_bA).$$

The second assertion follows immediately by construction since in the case that A is central, by definition of twisting using a cocycle, we have ${}_bA = A$ as groups over E . \square

Remark 2.3. The twisted forms \tilde{A} appeared in Proposition 2.2 are also smooth unipotent algebraic groups.

3. ESSENTIAL DIMENSION OF p -GROUPS IN CHARACTERISTIC p

In this section, using Proposition 2.2, we derive some corollaries concerning the essential dimension of finite étale group schemes of order p^n over a field of characteristic $p > 0$, see Proposition 3.1 and Proposition 3.5.

3.1. Upper bound for finite étale unipotent groups. The following result is obtained already by Ledet [Le] in the case that G is a finite abstract p -group, see also [TV, Theorem 1.4] for a more general result.

Proposition 3.1. *Let k be a field of characteristic p . Let G be a finite étale k -group scheme of order p^n . Then $\text{ed}_k(G) \leq n$.*

Proof. We proceed by induction on n . If $n = 1$ it is easy to see that $\text{ed}_k(G) = \text{ed}_k(\mathbb{Z}/p) = 1$ (for example, see [BF, page 292]). Now since $G(k^s)$ is a p -group, G has a central subgroup H of order p . By Proposition 2.2, we get

$$\text{ed}_k(G) \leq \text{ed}_k(H) + \text{ed}_k(G/H) = 1 + \text{ed}_k(G/H) \leq n,$$

since $\text{ed}_k(G/H) \leq n - 1$ by induction assumption. \square

Corollary 3.2. *Let k be a field of characteristic $p > 0$. Let*

$$1 \rightarrow P \rightarrow G \rightarrow A \rightarrow 1$$

be an exact sequence of finite étale k -group schemes. Assume that P is a finite étale k -group scheme of order p^n . Then

$$\mathrm{ed}_k(A) \leq \mathrm{ed}_k(G) \leq \mathrm{ed}_k(A) + n.$$

Proof. The first inequality follows from Lemma 2.1 and [BF, Lemma 1.9].

For the second inequality, let K/k be a field extension and x an element in $H^1(K, G)$. By Proposition 2.2, there is a subfield extension $k \subset E \subset K$ and a twisted form \tilde{P} of P_E such that

$$\mathrm{ed}(x) \leq \mathrm{ed}_k(A) + \mathrm{ed}_E(\tilde{P}).$$

By Proposition 3.1, $\mathrm{ed}_E(\tilde{P}) \leq n$ (note that the orders of \tilde{P} , of P_E and of P are all equal). Therefore, $\mathrm{ed}(x) \leq \mathrm{ed}_k(A) + n$ and hence $\mathrm{ed}_k(G) \leq \mathrm{ed}_k(A) + n$. \square

Remark 3.3. Without the assumption of being p -group on P , it is not true, in general, that $\mathrm{ed}_k(G) \geq \mathrm{ed}_k(G/P)$ (see [MZ, Theorem 1.5]).

3.2. Elementary p -groups. Let k be a field of characteristic $p > 0$. Let G be a finite étale k -group scheme. It is called an *elementary p -group scheme* (over k) if it is of p -power order, commutative and annihilated by p .

Lemma 3.4. *Let k be a field of characteristic $p > 0$, G an elementary finite étale p -group scheme over k . Then $\mathrm{ed}_k(G)$ is always less than or equal 2 and it is less than or equal 1 if k is infinite.*

Proof. If k is infinite then by Lemma 4.5 (in the next section), $\mathrm{ed}_k(G) \leq 1$.

Assume now that k is finite. Let $K \supset k$ be any field extension of k and a an arbitrary element in $H^1(K, G)$. We show that $\mathrm{ed}(a)$ is always less than or equal 2.

If $\mathrm{ed}(a) \leq 1$, then $\mathrm{ed}(a) < 2$ trivially.

If $\mathrm{ed}(a) \geq 1$ then there exist a field sub-extension $k \subset K_0 \subset K$ with $\mathrm{trdeg}_k(K_0) = \mathrm{ed}(a)$ and an element $x \in H^1(K_0, G)$ such that x is sent to a via $H^1(K_0, G) \rightarrow H^1(K, G)$. Since $\mathrm{trdeg}_k(K_0) = \mathrm{ed}(a) \geq 1$, K_0 contains $k(u)$, for some u , which is transcendental over k . Since $\mathrm{ed}_{k(u)}(G) \leq 1$, there is a subfield extension $k(u) \subset L \subset K_0$ with $\mathrm{trdeg}_{k(u)}(L) \leq 1$ and an element $y \in H^1(L, G)$ which is sent to x via $H^1(L, G) \rightarrow H^1(K_0, G)$. Then y is sent to a via $H^1(L, G) \rightarrow H^1(K, G)$. Therefore

$$\mathrm{ed}(a) \leq \mathrm{trdeg}_k(L) \leq 1 + 1 = 2.$$

So $\mathrm{ed}(a)$ is always less than or equal 2. Hence $\mathrm{ed}_k(G) \leq 2$. \square

3.3. Frattini subgroups. Recall that the *Frattini subgroup* $\Phi(G)$ of a abstract finite group G is the intersection of the maximal subgroups of G . It is a characteristic subgroup, i.e., it is invariant under every automorphism of G and if $G \neq 1$ then $\Phi(G) \neq G$. If G is p -group then $G/\Phi(G)$ is an elementary p -group.

To give a finite étale k -group scheme G is the same as to give a finite abstract group \mathbb{G} with a continuous action of $\mathrm{Gal}(k_s/k)$ where $\mathrm{Gal}(k_s/k)$ acts as group automorphisms.

Since the Frattini subgroup $\mathbb{H} = \Phi(\mathbb{G})$ of \mathbb{G} is invariant under the action of $\text{Gal}(k_s/k)$, \mathbb{H} with this Galois action defines a finite k -subgroup H of G , it is also called the Frattini subgroup of G . If G is a finite étale group scheme of order p^n , then G/H is an (finite étale) elementary p -group scheme over k .

We obtain the following result, which is Theorem 8.4.1 in [JLY] when G is an abstract p -group.

Proposition 3.5. *Let k be a field of characteristic $p > 0$, G a finite étale k -group scheme of order power of p and let the order of its Frattini subgroup $\Phi(G)$ be p^e .*

- (1) *If k is infinite then $\text{ed}_k(G) \leq e + 1$.*
- (2) *If k is finite then $\text{ed}_k(G) \leq e + 2$.*

Proof. We have the following exact sequence of finite étale k -group schemes

$$1 \rightarrow \Phi(G) \rightarrow G \rightarrow G/\Phi(G) \rightarrow 1,$$

with $N := G/\Phi(G)$ is an elementary p -group.

Let K/k be a field extension and x an element in $H^1(K, G)$. By Proposition 2.2, there is a subfield extension $k \subset E \subset K$ and a twisted form $\widetilde{\Phi(G)}$ of $\Phi(G)_E$ such that

$$\text{ed}(x) \leq \text{ed}_k(N) + \text{ed}_E(\widetilde{\Phi(G)}).$$

By Proposition 3.1, $\text{ed}_E(\widetilde{\Phi(G)}) \leq e$ (note that the order of $\widetilde{\Phi(G)}$ is equal to that of $\Phi(G)$). Therefore, $\text{ed}(x) \leq e + \text{ed}_k(N)$ and hence $\text{ed}_k(G) \leq e + \text{ed}_k(N)$. The corollary now follows from Lemma 3.4. \square

3.4. Homotopy invariance. In [BF, Section 8] they prove the so-called *homotopy invariance* of essential dimension, that is $\text{ed}_k(G) = \text{ed}_{k(t)}(G)$, for algebraic groups defined over infinite fields. In the next proposition, we show that this property does not hold for finite fields. Namely, we have

Proposition 3.6. *Let $k = \mathbb{F}_p$ and P an elementary p -group of rank ≥ 3 . Then*

$$\text{ed}_{k(t)}(P) < \text{ed}_k(P).$$

Proof. We consider P as a constant group scheme over k . By Lemma 4.5, $\text{ed}_{k(t)}(P) \leq 1$.

On the other hand, $\text{ed}_k(P) \geq 2$. In fact, assume for contradiction that $\text{ed}_k(P) \leq 1$ then P is isomorphic as an abstract group to a subgroup of $\text{PGL}_2(\mathbb{F}_p)$ (see for example [BF, Lemma 7.2]). But this cannot happen since

$$\text{Card}(G) \geq p^3 > p(p^2 - 1) = \text{Card}(\text{PGL}_2(\mathbb{F}_p)).$$

Therefore, $\text{ed}_k(P) > \text{ed}_{k(t)}(P)$. \square

4. UPPER BOUND FOR ESSENTIAL DIMENSION OF UNIPOTENT ALGEBRAIC GROUPS

In this section we will prove Theorem 1.1.

4.1. Tits' structure theory of unipotent algebraic groups. We first recall some results of Tits concerning the structure of unipotent algebraic groups over an arbitrary (especially imperfect) field of positive characteristic, see [Oe, Chapter V] and [CGP, Appendix B].

Let G be a smooth unipotent algebraic group over a field k of characteristic $p > 0$. Then there exists a maximal central smooth connected k -subgroup of G which is killed by p . This group is called *cckp-kernel* of G and denoted by $cckp(G)$ or $\kappa(G)$. Here $\dim(\kappa(G)) > 0$ if G is not finite.

The following statements are equivalent:

- (1) G is wound over k ,
- (2) $\kappa(G)$ is wound over k .

If the two equivalences are satisfied then $G/\kappa(G)$ is also wound over k ([Oe, Chapter V, 3.2]; [CGP, Appendix B, B.3]).

Proposition 4.1 (see [CGP, B.3.3]). *Let k be a field of characteristic $p > 0$. Let G be a k -wound smooth connected unipotent algebraic k -group. Define the ascending chain of smooth connected normal k -subgroups $\{G_i\}_{i \geq 0}$ as follows: $G_0 = 1$ and G_{i+1}/G_i is the cckp-kernel of the k -wound group G/G_i for all $i \geq 0$. These subgroups are stable under k -group automorphisms of G , their formation commutes with any separable extension of k , and $G_i = G$ for sufficiently large i .*

Definition 4.2. The smallest natural number i such that $G_i = G$ as in the previous proposition is called *the cckp-kernel length* of G and denoted by $l = lcckp(G)$.

Note that $lcckp(G) \leq \dim G$ since the cckp-kernel of a non-trivial smooth connected unipotent algebraic k -group is non-trivial.

Definition 4.3. Let k be a field of characteristic $p > 0$. A polynomial $P \in k[T_1, \dots, T_r]$ is a *p -polynomial* if every monomial appearing in P has the form $c_{ij}T_i^{p^j}$ for some $c_{ij} \in k$; that is $P = \sum_{i=1}^r P_i(T_i)$ with $P_i(T_i) = \sum_j c_{ij}T_i^{p^j} \in k[T_i]$.

A p -polynomial $P \in k[T_1, \dots, T_r]$ is called *separable* if it contains at least a non-zero monomial of degree 1.

If $P = \sum_{i=1}^r P_i(T_i)$ is a p -polynomial over k in r variables, then the *principal part* of P is the sum of the leading terms of the P_i .

Proposition 4.4 (see [Oe, Ch. V, 6.3, Proposition] and [CGP, Proposition B.1.13]). *Let k be an infinite field of characteristic $p > 0$. Let G be a smooth unipotent algebraic k -group of dimension n . Assume that G is commutative and annihilated by p . Then G is isomorphic (as a k -group) to the zero scheme of a separable nonzero p -polynomial over k , whose principal part vanishes nowhere over $k^{n+1} \setminus \{0\}$.*

4.2. Smooth connected unipotent algebraic groups. In this section we give an upper bound for essential dimension of smooth connected algebraic groups, see Theorem 4.6.

Lemma 4.5. *Let k be an infinite field of characteristic $p > 0$. Let G be a smooth unipotent algebraic k -group. Assume that G is commutative and annihilated by p . Then $\text{ed}_k(G) \leq 1$.*

Proof. By a result of Tits (see Proposition 4.4), G is isomorphic (as a k -group) to the zero scheme of a separable nonzero p -polynomial $f(T_1, \dots, T_n)$, where $n = \dim G + 1$, over k . That means we have the following exact sequence of k -groups

$$0 \rightarrow G \rightarrow \mathbb{G}_a^n \xrightarrow{f} \mathbb{G}_a \rightarrow 0.$$

This follows that $H^1(K, G) = K/f(K)$ for any field extension K/k and hence $\text{ed}_k(G) \leq 1$. \square

Theorem 4.6. *Let G be a smooth connected algebraic unipotent group over a field k of characteristic $p > 0$, G_s the k -split part of G . Let l be the cckp-kernel length of G/G_s . Then $\text{ed}_k(G) \leq l$.*

Proof. If k is finite then G is k -split and hence $\text{ed}_k(G) = 0 \leq l$.

Now we assume that k is infinite. By Lemma 2.1, the natural map $H^1(K, G) \rightarrow H^1(K, G/G_s)$ is a bijection for all field $K \supset k$. Therefore, $\text{ed}_k(G) = \text{ed}(G/G_s)$. Set $H = G/G_s$ and let $\{H_i\}_{i \geq 0}$ be the ascending chain of normal subgroups of H as in Proposition 4.1 with $l = \text{lcckp}(H)$.

Since H_{i+1}/H_i is the cckp-kernel of H/H_i , in particular, it is commutative and killed by p . Therefore, by Lemma 4.5, $\text{ed}_k(H_{i+1}/H_i) \leq 1$. Applying Proposition 2.2 to the following exact sequence

$$1 \rightarrow H_{i+1}/H_i \rightarrow H/H_i \rightarrow H/H_{i+1} \rightarrow 1,$$

one has

$$\text{ed}_k(H/H_i) \leq \text{ed}_k(H/H_{i+1}) + 1,$$

for all $i = 0, \dots, l = \text{lcckp}(H)$. It implies that

$$\text{ed}_k(H) = \text{ed}_k(H/H_0) \leq \text{ed}_k(H/H_l) + l = l,$$

as required. \square

The following result can be considered as a counterpart of Proposition 3.1 for smooth connected unipotent algebraic groups.

Corollary 4.7. *Let G be a smooth connected unipotent algebraic group over a field k of characteristic $p > 0$. Then $\text{ed}_k(G) \leq \dim G$.*

Proof. Let G_s be the k -split part of G , l the cckp-kernel of G/G_s . By Theorem 4.6, $\text{ed}_k(G) \leq l$. The corollary then follows from the fact that cckp-kernel length l of G/G_s is less than or equal $\dim G/G_s \leq \dim G$. \square

Remark 4.8. Corollary 4.7 can also be proved by induction on $\dim G$ as follows: It is enough to consider the case k is infinite. Assume that this is the case. If $\dim G = 1$, then G is commutative and annihilated by p . Thus $\text{ed}_k(G) \leq 1$ by Lemma 4.5. Assume that $\dim G > 1$. By [TT2, Proposition 1], there exists a normal smooth connected k -subgroup H of codimension 1 in G . Consider the following exact sequence

$$1 \rightarrow H \rightarrow G \rightarrow G/H \rightarrow 1.$$

Let K/k be a field extension and x an element in $H^1(K, G)$. By Proposition 2.2, there is a subfield extension $k \subset E \subset K$ and a twisted form \tilde{H} of H_E such that

$$\text{ed}(x) \leq \text{ed}_k(G/H) + \text{ed}_E(\tilde{H}).$$

By induction assumption, one has $\text{ed}_E(\tilde{H}) \leq \dim \tilde{H} = \dim H$. Therefore $\text{ed}(x) \leq 1 + \dim H = \dim G$ and hence $\text{ed}_k(G) \leq \dim G$.

Remark 4.9. Fix a natural number n , Ledet conjectures that $\text{ed}_k(\mathbb{Z}/p^n\mathbb{Z}) = n$ over any field k of characteristic p . However, to the author's knowledge, there are no candidates for smooth connected unipotent algebraic groups and fields with the essential dimension n . We would like to raise the following question.

Question 4.10. For any natural number n , does there exist a field k and a smooth connected unipotent k -group G such that $\text{ed}_k(G) = n$?

4.3. Proof of Theorem 1.1. By Lemma 2.1, one has $\text{ed}_k(G) = \text{ed}_k(H)$. If $\text{char } k = 0$ then it is well-known that G is k -split, i.e., $H = G/G_s$ is trivial. Hence $\text{ed}_k(G) = 0$ and the theorem holds trivially.

We now assume that k is of characteristic $p > 0$. We consider the following exact sequence of k -groups

$$1 \rightarrow H^0 \rightarrow H \rightarrow H/H^0 \rightarrow 1.$$

Let K/k be a field extension and x an element in $H^1(K, H)$. Then by Proposition 2.2, there is a subfield extension $k \subset E \subset K$ and a twisted form \tilde{H}^0 of H_E^0 such that

$$\text{ed}(x) \leq \text{ed}_k(H/H^0) + \text{ed}_E(\tilde{H}^0).$$

By Corollary 4.7,

$$\text{ed}_k(\tilde{H}^0) \leq \dim \tilde{H}^0 = \dim H_E^0 = \dim G/G_s.$$

Hence, we have the first inequality

$$\text{ed}_k(G) \leq \text{ed}_k(H/H^0) + \dim(G/G_s).$$

The second inequality follows immediately from Proposition 3.1. \square

5. IMAGES OF ADDITIVE POLYNOMIALS OVER VALUED FIELDS

In this section, we prove a result concerning the image of an additive polynomial over certain valued field, see Proposition 5.10, which is needed in proving Theorem 1.2 in Section 6.

5.1. Some lemmas.

Lemma 5.1. *Let Γ be a nontrivial totally ordered commutative group*

- (1) *For any element γ in Γ , there exists $\beta \in \Gamma$ such that $\beta < \gamma$.*
- (2) *Let $\gamma_1, \dots, \gamma_r$ be elements in Γ and let n_1, \dots, n_r be positive numbers. Then there exists an element γ_0 in Γ such that for all elements $\gamma < \gamma_0$, $\gamma \in \Gamma$, we have $n_i \gamma < \gamma_i$ for all i .*

Proof. 1) If $\gamma \geq 0$, then let $\beta < 0 \leq \gamma$ (such an element exists since Γ is nontrivial).

If $\gamma < 0$, one can take $\beta = 2\gamma < \gamma$.

2) We set

$$\gamma_0 := \min\{\gamma_1, \dots, \gamma_r, 0\}.$$

Now let γ be an arbitrary element such that $\gamma < \gamma_0$. Since $\gamma < \gamma_i$, $\gamma < 0$, it follows that $n_i\gamma < \gamma_i$, for all i . \square

Lemma 5.2. *Let Γ be a totally ordered commutative group, p a prime number, d a natural number. Let α_0, γ_0 be elements in Γ . Then there exist infinitely many elements $\gamma_i \in \Gamma$ such that*

$$\gamma_0 > \gamma_1 > \dots > \gamma_i > \dots$$

and $\gamma_i \equiv \alpha_0$ modulo p^d for all $i > 0$.

Proof. By Lemma 5.1, there is $\gamma \in \Gamma$ such that $p^d\gamma < \gamma_0 - \alpha$. We set $\gamma_1 := \alpha + p^d\gamma$. Then $\gamma_1 < \gamma_0$ and $\gamma_1 \equiv \alpha_0$ modulo p^d . Continuing this way, one can construct a sequence $\gamma_0 > \gamma_1 > \gamma_2 > \dots$ satisfies the requirement of the lemma. \square

The following lemma is a generalization of [TT1, Lemma 4.4.1] from discrete valuation to arbitrary valuation. Using some modifications, the proof in [TT1] works well in our case. Because the proof is quite technical, we would like to give it here in detail for reader's convinence.

Lemma 5.3. *Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k with the value group Γ . Let $P = \sum_{i=1}^r \sum_j c_{ij} T_i^{p^j}$ a non-trivial p -polynomials in r variables with coefficients in k . Let $P_{\text{princ}} = \sum_{i=1}^r c_i T_i^{p^{m_i}}$ be the principal part of P . Assume that for all $(a_1, \dots, a_r) \in k \times \dots \times k$ (r times), $v(c_i) + p^{m_i}v(a_i)$ are all distinct whenever they are defined. Then there exists a constant C_0 depending only on P such that if $a = P(a_1, \dots, a_r)$ and $v(a) < C_0$ then $v(a) = v(c_i) + p^{m_i}v(a_i)$, for some i .*

Proof. We process by induction on r . First let $r = 1$, $P(T) = b_0T + \dots + b_mT^{p^m}$, $b_m \neq 0$. Set $I := \{i \mid b_i \neq 0\} \subset \{0, \dots, n\}$. By Lemma 5.1, there exists $A \in \Gamma$ such that

$$(p^m - p^i)A < v(b_i) - v(b_m), \forall i \in I \setminus \{m\}.$$

We set

$$B = \min_{i \in I} \{Ap^i + v(b_i)\},$$

and pick any C_0 with $C_0 < B$. Now assume that $a = P(a_1)$ ($a_1 \in k$) such that $v(a) \leq C_0$. Let i_0 be such that

$$v(b_{i_0}a_1^{p^{i_0}}) = \min_{i \in I} \{v(b_i a_1^{p^i})\}.$$

Then we have $C_0 \geq v(a) = v(P(a_1)) \geq v(b_{i_0}a_1^{p^{i_0}}) = v(b_{i_0}) + p^{i_0}v(a_1)$. Hence by the choices of C_0 and of B , one has

$$p^{i_0}v(a_1) \leq C_0 - v(b_{i_0}) < B - v(b_{i_0}) \leq Ap^{i_0}.$$

This implies that $v(a_1) < A$ and by the definition of A ,

$$(p^m - p^i)v(a_1) < v(b_i) - v(b_m), \forall i \in I \setminus \{m\},$$

or equivalently,

$$v(b_i a_1^{p^i}) = v(b_i) + p^i v(a_1) > v(b_m) + p^m v(a_1) = v(b_m a_1^{p^m}), \forall i \in I \setminus \{m\}.$$

Therefore $v(a) = v(b_m) + p^m v(a_1)$ as required.

Now assume that $r > 1$ and that the assertion of the lemma holds true for all integers less than r . By induction hypothesis, for any l with $1 \leq l < r$, there exist constants B_l (in the value group Γ) satisfying the lemma for the case $r = l$. Any monomial of $P(T_1, \dots, T_r) - P_{\text{princ}}(T_1, \dots, T_r)$ is of the form $\lambda T_j^{p^{m_j-s}}$ with $\lambda \in k^\times$, $1 \leq j \leq r$, $1 \leq s$, and for such a monomial we choose an element $a_{\lambda,s,j}$ in Γ such that

$$(p^{m_j} - p^{m_j-s})a_{\lambda,s,j} < v(\lambda) - v(c_j).$$

(The existence of such an element is ensured by Lemma 5.1.) Also by Lemma 5.1, we can choose C_3 and C_2 in Γ such that

$$\begin{aligned} p^{m_i} C_3 &< v(\lambda) + p^{m_j-s} a_{\lambda,j,s} - v(c_i), \forall \lambda, j, s; \\ p^{m_j} C_2 &< v(c_i) + p^{m_i} C_3 - v(c_j), \forall i, j. \end{aligned}$$

Let

$$\begin{aligned} C_1 &= \min_{i,j} \{v(c_{ij}) + p^j C_2\}, \\ C_0 &= \min\{C_1, B_1, \dots, B_{r-1}\}. \end{aligned}$$

Assume that $a = P(a_1, \dots, a_r)$, $a_i \in k$ and $v(a) < C_0$. If there exists i such that $a_i = 0$ then the cardinality of the set $\{i \mid a_i \neq 0\}$ is less than r and instead of P we can consider the polynomial

$$\tilde{P} = P(T_1, \dots, T_{i-1}, 0, T_{i+1}, \dots, T_r)$$

in $r-1$ variables and use the induction hypothesis. So we assume that $a_i \neq 0$ for all i . Let

$$i_0 = \min_{1 \leq i \leq r} \{i \mid v(a_i) \leq v(a_j), \text{ for all } j, 1 \leq j \leq r\}.$$

Then

$$v(a) = v(P(a_1, \dots, a_r)) \geq \min\{v(c_{ij} a_i^{p^j})\} \geq \min\{v(c_{ij}) + p^j v(a_{i_0})\}.$$

By assumption $v(a) < C_0 \leq C_1$, that implies that, for some i, j , one has

$$v(c_{ij}) + p^j v(a_{i_0}) < C_1 \leq v(c_{ij}) + p^j C_2.$$

Hence $v(a_{i_0}) < C_2$. Since $v(c_i) + p^{m_i} v(a_i)$ are pairwise distinct, there exists a unique i_1 such that

$$v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}) = \min_{1 \leq j \leq r} \{v(c_j) + p^{m_j} v(a_j)\}.$$

Since

$$v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}) \leq v(c_{i_0}) + p^{m_{i_0}} v(a_{i_0}) < v(c_{i_0}) + p^{m_{i_0}} C_2,$$

one has $v(a_{i_1}) < C_3$, since otherwise we would have

$$v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}) \geq v(c_{i_1}) + p^{m_{i_1}} C_3 \geq v(c_{i_0}) + p^{m_{i_0}} C_2$$

which contradicts the above inequalities.

Now we show that

$$v(P(a_1, \dots, a_r)) = v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}).$$

This follows from two facts below:

(i) For any monomial $\lambda T_j^{p^{m_j-s}}$ of $P(T_1, \dots, T_r) - P_{\text{princ}}(T_1, \dots, T_r)$, $\lambda \in k^\times$, $1 \leq j \leq r$, $1 \leq s$, if $v(a_j) < a_{\lambda,j,s}$ then by the definitions of $a_{\lambda,j,s}$ and of i_1 one has

$$v(\lambda a_j^{p^{m_j-s}}) = v(\lambda) + p^{m_j-s}v(a_j) > v(c_j) + p^{m_j}v(a_j) \geq v(c_{i_1}) + p^{m_1}v(a_{i_1}).$$

Also, if $v(a_j) \geq a_{\lambda,j,s}$ then again by definitions of $a_{\lambda,j,s}$ and of C_s one has

$$v(\lambda a_j^{p^{m_j-s}}) \geq v(\lambda) + p^{m_j-s}a_{\lambda,j,s} > v(c_{i_1}) + p^{m_{i_1}}C_3 > v(c_{i_1}) + p^{m_{i_1}}v(a_{i_1}),$$

since $v(a_{i_1}) < C_3$.

Thus one always has

$$v(\lambda a_j^{p^{m_j-s}}) > v(c_{i_1}) + p^{m_1}v(a_{i_1}).$$

(ii) For $j \neq i_1$, by the uniqueness of i_1 one has

$$v(c_j a_j^{p^{m_j}}) > v(c_{i_1}) + p^{m_{i_1}}v(a_{i_1}).$$

Hence

$$v(P_{\text{princ}}(a_1, \dots, a_r)) = v\left(c_{i_1} a_{i_1}^{p^{m_{i_1}}} + \sum_{j \neq i_1} c_j a_j^{p^{m_j}}\right) = v(c_{i_1} a_{i_1}^{p^{m_{i_1}}}).$$

Now (i) and (ii) imply that

$$\begin{aligned} v(a) &= v(P(a_1, \dots, a_r)) \\ &= v(P_{\text{princ}}(a_1, \dots, a_r) + (P(a_1, \dots, a_r) - P_{\text{princ}}(a_1, \dots, a_r))) \\ &= v(c_{i_1} a_{i_1}^{p^{m_{i_1}}}) = v(c_{i_1}) + p^{m_{i_1}}v(a_{i_1}). \end{aligned}$$

The proof of the lemma is completed. \square

5.2. Valuation basis.

Definition 5.4. Let (k, v) be a valued field of characteristic $p > 0$, d a natural number. A system $(b_i)_{i \in I}$ of non-zero elements in k is called k^{p^d} -valuation independent with respect to (w.r.t) the valuation v if the values $v(b_i)$, $i \in I$ are all pairwise distinct modulo p^d .

If V a k^{p^d} -vector subspace of k , this system is called *valuation basis* of V if it generates V as k^{p^d} -vector space and it is k^{p^d} -valuation independent.

Remarks 5.5. (1) Notations being as above. If $(b_i)_{i \in I}$ is k^{p^d} -valuation independent then it is k^{p^d} -linearly independent (see the proof of Lemma 5.6 (2) below). In particular, a valuation basis of V is a basis of V as k^{p^d} -vector space.

(2) Our definitions of valuation independence and of valuation basis are slightly different from those in [DK]. A valuation basis in our sense is a valuation basis in their sense.

Lemma 5.6. Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k . Let n, d be natural numbers.

- (1) Suppose that there are n elements of k which are k^p -valuation independent with respect to v . Then there are n^d elements which are k^{p^d} -valuation independent with respect to v .

- (2) If k has a finite k^p -valuation basis with respect to v then k has a finite k^{p^d} -valuation basis with respect to v .

Proof. (1) We process by induction on d . By assumption, the statement (1) is true for $d = 1$.

Now we assume that $d \geq 2$ and that the assertion of (1) is true for $d - 1$, i.e., there is a $k^{p^{d-1}}$ -basis $g_1, \dots, g_{n^{d-1}}$ such that $v(g_1), \dots, v(g_{n^{d-1}})$ are pairwise distinct modulo p^{d-1} .

Let e_1, \dots, e_n be elements of k such that $v(e_1), \dots, v(e_n)$ are pairwise distinct modulo p .

For each pair i, j with $1 \leq i \leq n^{d-1}, 1 \leq j \leq n$ we define $u_{ij} = g_i e_j^{p^{d-1}}$. Then there are n^d such of u_{ij} and these $v(u_{ij})$ are pairwise distinct modulo p^d . In fact, if $v(u_{ij}) \equiv v(u_{i'j'})$ modulo p^d for two pairs (i, j) and (i', j') then

$$v(g_i) - v(g_{i'}) + p^{d-1}(v(e_j) - v(e_{j'})) \equiv 0 \pmod{p^d}.$$

In particular $v(g_i) - v(g_{i'}) \equiv 0 \pmod{p}$, hence $i = i'$. This implies that $v(e_j) - v(e_{j'}) \equiv 0 \pmod{p}$ and $j = j'$.

(2) We first note that such u_{ij} are k^{p^d} -linear independent. In fact, assume that there is a non-trivial k^{p^d} -linear combination $\sum a_{ij}^{p^d} u_{ij} = 0$. Since all value $v(a_{ij}^{p^d} u_{ij}) = p^d v(a_{ij}) + v(u_{ij})$ are pairwise distinct whenever they are defined, one has

$$v(0) = v\left(\sum a_{ij}^{p^d} u_{ij}\right) = p^d v(a_{i_0 j_0}) + v(u_{i_0 j_0}),$$

for some pair (i_0, j_0) , it is impossible.

Now (2) follows from the part (1) and the fact that $[k : k^{p^d}] = [k : k^p]^d$ (by induction on d). \square

Lemma 5.7. *Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k and let d be a natural number. We assume that k has a finite k^{p^d} -valuation basis with respect to v . Let V be a k^{p^d} -vector subspace of k . Then V has a (finite) k^{p^d} -valuation basis with respect to v .*

Proof. Let $N = [k : k^{p^d}]$ and u_1, \dots, u_N a k^{p^d} -valuation basis of k . Let b_1, \dots, b_s be a k^{p^d} -basis of V . Then for each i , we can write

$$b_i = a_{i1}^{p^d} u_1 + \dots + a_{iN}^{p^d} u_N,$$

where a_{ij} are elements in k . Since $v(u_j)$ are pairwise distinct modulo p^d , the values $v(a_{ij}^{p^d} u_j)$ are pairwise distinct. Hence there is a unique index j_1 such that $v(b_1) = v(a_{1j_1}^{p^d} u_{j_1})$. In particular $a_{1j_1} \neq 0$.

We set $b'_1 := b_1$ and for each $i \geq 2$, we set $b'_i := b_i - (a_{ij_1}/a_{1j_1})^{p^d} b_1$. Then b'_1, \dots, b'_s form a k^{p^d} -basis of V . Moreover, terms of the form $\lambda^{p^d} u_{j_1}$ do not appear in b'_2, \dots, b'_s . Similarly, for each $i \geq 2$, we can write

$$b'_i = (a'_{i1})^{p^d} u_1 + \dots + (a'_{iN})^{p^d} u_N,$$

where a'_{ij} are elements in k . And there is a unique index j_2 such that $v(b'_2) = v((a'_{ij_1})^{p^d} u_{j_2})$. We set $b''_2 := b'_2$ and $b''_i := b'_i - (a'_{ij_2}/a'_{2j_2})^{p^d} b'_2$. Note that $j_2 \neq j_1$ and terms of forms $\lambda_1^{p^d} u_{j_1}$ and of forms $\lambda_2^{p^d} u_{j_2}$ do not appear in b''_3, \dots, b''_s .

Continuing this way by modifying b''_3, \dots, b''_s and so on, we obtain a k^{p^d} -basis c_1, \dots, c_s of V such that $v(c_1), \dots, v(c_s)$ are pairwise distinct modulo p^d . \square

5.3. A lemma of Dries and Kuhlmann. The following lemma is a generalization of [DK, Lemma 4]. They treat the case of local fields, i.e., complete discrete valued fields with finite residue field. With the help of Lemma 5.7, their proof can be extended to our case. We include it here for the reader's convenience.

Lemma 5.8. *Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k . We assume that k has a finite k^p -valuation basis. Let $P = f_1(T_1) + \dots + f_r(T_r)$ be an additive (i.e. p -) polynomial with coefficients in k in r variables, the principal part of which vanishes nowhere over $k^r \setminus \{0\}$. Let $S = \text{im}(P) = f_1(k) + \dots + f_r(k)$. Let $p^{d_i} = \deg f_i$, $p^d = \max p^{d_i}$, and $s = \sum_{i=1}^r n^{d-d_i}$ where $n := [k : k^p]$. Then there are s additive polynomials $g_1, \dots, g_s \in k[X]$ in one variable X such that*

- (1) $S = g_1(k) + \dots + g_s(k)$;
- (2) all polynomials g_i have the same degree p^d ;
- (3) the leading coefficients b_1, \dots, b_s of g_1, \dots, g_s are such that $v(b_1), \dots, v(b_s)$ are distinct modulo p^d .

Proof. By Lemma 5.6, for each i , there are n^{d-d_i} elements $u_{i1}, \dots, u_{i,n^{d-d_i}}$ such that these elements form a $k^{p^{d-d_i}}$ -basis of k and $v(u_{i1}), \dots, v(u_{i,n^{d-d_i}})$ are pairwise distinct modulo p^{d-d_i} . In particular, we can write

$$k = u_{i1} k^{p^{d-d_i}} + \dots + u_{i,n^{d-d_i}} k^{p^{d-d_i}}.$$

Hence

$$f_i(k) = f_i(u_{i1} k^{p^{d-d_i}}) + \dots + f_i(u_{i,n^{d-d_i}} k^{p^{d-d_i}}) = h_{i1}(k) + \dots + h_{i,n^{d-d_i}}(k)$$

where

$$h_{ij}(X) := f_i(u_{ij} X^{p^{d-d_i}}) \in k[X].$$

And then

$$S = \sum_{i=1}^r \sum_{j=1}^{n^{d-d_i}} h_{ij}(k)$$

with all polynomials h_{ij} having degree p^d .

We claim that the leading coefficients $c_{ij} = c_i u_{ij}^{p^{d_i}}$ of the polynomials h_{ij} are k^{p^d} -linearly independent. In fact, assume that for $a_{ij} \in k$,

$$0 = \sum_{i=1}^r \sum_{j=1}^{n^{d-d_i}} c_{ij} a_{ij}^{p^d} = \sum_{i=1}^r c_i \sum_{j=1}^{n^{d-d_i}} u_{ij}^{p^{d_i}} a_{ij}^{p^d} = \sum_{i=1}^r c_i \left(\sum_{j=1}^{n^{d-d_i}} u_{ij} a_{ij}^{p^{d-d_i}} \right)^{p^{d_i}}.$$

By assumption that the principal part of P vanishes nowhere over $k^r \setminus \{0\}$, one has

$$\sum_{j=1}^{n^{d-d_i}} u_{ij} a_{ij}^{p^{d-d_i}} = 0 \quad \text{for } 1 \leq i \leq r.$$

Since $u_{i1}, \dots, u_{i, n^{d-d_i}}$ are $k^{p^{d-d_i}}$ -linearly independent, $a_{ij} = 0$ for all i and j .

We have now found $s = \sum_{i=1}^r n^{d-d_i}$ additive (i.e., p -) polynomials $\tilde{h}_1, \dots, \tilde{h}_s$ in $k[X]$ with k^{p^d} -linearly independent leading coefficients $\tilde{c}_1, \dots, \tilde{c}_s$ and such that $S = \tilde{h}_1(k) + \dots + \tilde{h}_s(k)$. The Lemma 5.7 shows that the k^{p^d} -vector space generated by $\tilde{c}_1, \dots, \tilde{c}_s$ admits a k^{p^d} -basis b_1, \dots, b_s , say, for which $v(b_1), \dots, v(b_s)$ are pairwise distinct modulo p^d . Write $b_i = \sum_{j=1}^s r_{ij}^{p^d} \tilde{c}_j$ and we set

$$g_i(X) := \sum_{j=1}^s \tilde{h}_j(r_{ij} X)$$

and observe that for each i the polynomial g_i is of degree p^d with leading coefficient b_i .

It only remains to show that the condition (1) is satisfied. Since S is an additive subgroup of K and contains the images $\tilde{h}_j(k)$ for all j it follows that

$$g_1(k) + \dots + g_s(k) \subset \tilde{h}_1(k) + \dots + \tilde{h}_s(k) = S.$$

On the other hand, both $\tilde{c}_1, \dots, \tilde{c}_s$ and b_1, \dots, b_s are bases, so the matrix $(r_{ij}^{p^d})$ is invertible. Hence, the matrix (r_{ij}) is also invertible. Denote its inverse by (s_{ij}) , with $s_{ij} \in k$. One can check that

$$\tilde{h}_i = \sum_{j=1}^s g_j(s_{ij} X).$$

Hence $S = \tilde{h}_1(k) + \dots + \tilde{h}_s(k) \subset g_1(k) + \dots + g_s(k)$, which concludes the proof. \square

5.4. Images of p -polynomials.

Lemma 5.9. *Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k with value group Γ . Assume that k has a finite k^p -valuation basis then we have*

$$[k : k^p] = [\Gamma : p\Gamma] = p^m,$$

for some natural number m .

Proof. Let $N = [k : k^p]$. Consider a finite set of elements $\gamma_1, \dots, \gamma_{N'}$, $\gamma_i \in \Gamma$, which are representatives of cosets of $p\Gamma$ in Γ . For each i , choose an element $b_i \in k$ such that $v(b_i) = \gamma_i$. As $v(b_1), \dots, v(b_{N'})$ are pairwise distinct modulo p , it implies that $b_1, \dots, b_{N'}$ are k^p -linearly independent. In particular $N' \leq N$. Hence $[\Gamma : p\Gamma]$ is finite and $M := [\Gamma : p\Gamma] \leq N$.

On the other hand, let e_1, \dots, e_N a k^p -valuation basis of p . Since $v(e_1), \dots, v(e_N)$ are pairwise distinct modulo p , we have $N \leq M$. Therefore $N = M$.

Finally, note that k/k^p is a finite \mathbb{F}_p -vector space, so $N = p^m$, for some m . \square

Now we have the following result, which plays an important role in the proof of Theorem 1.2 in the last section.

Proposition 5.10. *Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k with value group Γ . We assume that k has a finite k^p -valuation basis and set $p^m := [k : k^p]$. Let P be a p -polynomial in r variables with coefficients in k satisfying the condition that the principal part $P_{\text{princ}} = \sum_{i=1}^r c_i T_i^{p^{m_i}}$, $c_i \in k^*$, vanishes nowhere over $k^r \setminus \{0\}$. Let $d = \max m_i$. Then we have*

$$s := \sum_{i=1}^r p^{m(d-m_i)} \leq p^{md}.$$

Furthermore, if $s < p^{md}$ then the quotient $k/P(k)$ is infinite.

Proof. We write

$$P(T_1, \dots, T_r) = f_1(T_1) + \dots + f_r(T_r),$$

where each f_i is a p -polynomial in one variable T_i with coefficients in k and of degree p^{m_i} . We set

$$S = \text{im}(P) = f_1(k) + \dots + f_r(k).$$

Choose g_1, \dots, g_s with leading coefficients b_1, \dots, b_s , for which $v(b_1), \dots, v(b_s)$ are pairwise distinct modulo p^d as in Lemma 5.8. We set

$$Q(T_1, \dots, T_s) = g_1(k) + \dots + g_s(k).$$

Then $S = \text{im}(Q)$.

By Lemma 5.9, $\Gamma/p\Gamma$ is of order p^m and $\Gamma/p^d\Gamma$ is of order p^{md} by induction on d . As $v(b_1), \dots, v(b_s)$ are pairwise distinct modulo p^d , it implies in particular that $s \leq p^{md}$.

Now we assume that $s < p^{md}$. Then there is an element $l \in \Gamma$ such that $v(b_i) \not\equiv l \pmod{p^d}$ for all $i \in \{1, \dots, s\}$.

Since $v(b_1), \dots, v(b_s)$ are pairwise distinct modulo p^d , for any tuple $(a_1, \dots, a_s) \in k^\times \times \dots \times k^\times$ (s times), the values $v(b_i) + p^d v(a_i)$, $1 \leq i \leq s$, are pairwise distinct. Then all conditions in Lemma 5.3 are satisfied (for the p -polynomial Q), so there is C_0 as in the lemma.

We claim that for all $a \in k$ with $v(a) \leq C_0$ and $v(a) \equiv l \pmod{p^d}$, a is not in $S = \text{im}Q$. In fact, assume that $a = Q(a_1, \dots, a_s)$. By Lemma 5.3, there is an index i such that $v(a) = v(b_i) + p^d v(a_i)$. But this contradicts to the fact that $v(b_i) \not\equiv l \pmod{p^d}$, hence the claim follows.

By Lemma 5.2, we can choose a sequence $(e_i)_i$, $e_i \in k$ for all $i \geq 1$ such that

$$C_0 > v(e_1) > v(e_2) > \dots > v(e_i) > \dots$$

and $v(e_i) \equiv l \pmod{p^d}$ for all i . Then $v(e_i - e_{i+j}) = v(e_{i+j}) \equiv l \pmod{p^d}$ for all $i, j \geq 1$. By the claim above, $e_i - e_{i+j} \notin \text{im}(Q) = S$ for all $i, j \geq 1$. Hence all e_i have distinct images in $k/\text{im}(Q) = k/\text{im}(P)$. Therefore $k/\text{im}(P)$ is infinite as required. \square

6. UNIPOTENT GROUPS OF ESSENTIAL DIMENSION 0

In this section, we will prove Theorem 1.2 and Corollary 1.3 stated in the Introduction.

6.1. Infiniteness of Galois cohomology of unipotent algebraic groups over valued fields.

Proposition 6.1. *Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k . We assume that k has a finite k^p -valuation basis (see Definition 5.4). Let G a non-trivial smooth connected unipotent algebraic k -group of dimension $< [k : k^p] - 1$. If G is not split over k then $H^1(k, G)$ is infinite.*

Proof. Let G_s be the k -split part of G . Then G/G_s is nontrivial, connected, k -wound and $H^1(k, G) = H^1(k, G/G_s)$ by Lemma 2.1. So we may assume that G is wound over k . By [Oe, Chapter V, 3.3], G has a composition series of characteristic subgroups defined and wound over k : $G = G_0 \supset G_1 \supset \cdots \supset G_u = 1$ such that each quotient G_i/G_{i+1} is commutative, k -wound and annihilated by p . Also by Lemma 2.1, we may assume further that G is commutative, wound over k and annihilated by p . In this case, G is k -isomorphic to a k -subgroup of \mathbb{G}_a^r , where $r = \dim G + 1$, which is the zero set of a separable p -polynomial $P(T_1, \dots, T_r) \in k[T_1, \dots, T_r]$, whose the principal part $P_{\text{princ}} = \sum_{i=1}^r c_i T_i^{p^{m_i}}$ vanishes nowhere over $k^r \setminus \{0\}$, see Proposition 4.4.

By Proposition 5.10, one has

$$s := \sum_{i=1}^r p^{m(d-m_i)} \leq p^{md},$$

where $d := \max m_i$ and $p^m := [k : k^p]$.

Assume that $s = p^{md}$. Then one has

$$p^{md} - 1 = s - 1 = \sum_{i=1}^r (p^{m(d-d_i)} - 1) + (r - 1).$$

This implies that $r - 1 = \dim G$ is divisible by $p^m - 1$, and hence $\dim G \geq p^m - 1$ (note that G is nontrivial and connected, so $\dim G > 0$). This contradicts to the assumption that $\dim G < p^m - 1$. Therefore, $s < p^{md}$ and by Proposition 5.10, $H^1(k, G)$ is infinite. \square

6.2. Weil restriction. To prove Theorem 1.2, we also need some basic facts about Weil restriction of linear algebraic groups over fields (equivalently, smooth affine group schemes over fields) as presented in [Oe, Appendices A.2-A.3].

Let $\rho : k \rightarrow k'$ be a homomorphism of commutative rings, where k' is a projective k -module of finite type. For any affine k -scheme W' we then can associate an affine k -scheme $\mathcal{R}_{k'/k} W'$ called the Weil restriction of W' , which satisfies the following universal property: for any k -scheme V , one has a bijection (functorial in V)

$$\text{Hom}_{k\text{-sch}}(V, \mathcal{R}_{k'/k} W') \rightarrow \text{Hom}_{k'\text{-sch}}(V \times_k k', W').$$

We refer the reader to the [BLR, Chapter 7, 7.6] for a more general study of Weil restriction.

Lemma 6.2. *Let $\rho : k \rightarrow k'$ be a finite field extension and G' be a linear algebraic group over k' . Let $G = \mathcal{R}_{k'/k} G'$ be its Weil restriction. The following properties are true.*

- (1) G is a linear algebraic group and $H^1(k, G) \simeq H^1(k', G')$.

- (2) G is connected (resp. unipotent) if and only if G' is connected (resp. unipotent).
- (3) G is unipotent and k -wound if and only if G' is unipotent and k' -wound.
- (4) G is unipotent and k -split if and only if G' is unipotent and k' -split.

Proof. (1) These follow from [Oe, Appendix 3, A.3.2] and [Oe, Chapter IV, 2.3, Corollary].

(2) This is [Oe, Appendix 3, A.3.7].

(3) By the definition of Weil restriction, one has

$$\begin{aligned} G(k[[T]]) &\simeq G'(k[[T]] \otimes_k k') \simeq G'(k'[[T]]), \\ G(k((T))) &\simeq G'(k((T)) \otimes_k k') \simeq G'(k'((T))), \end{aligned}$$

where $k[[T]]$, resp. $k'[[T]]$, is the ring of formal power series in one variable T over k , resp. k' and $k((T))$, resp. $k'((T))$, is the fraction of $k[[T]]$, resp. $k'[[T]]$ and all isomorphisms appeared are canonical. (Note that two canonical maps $k[[t]] \otimes_k k' \simeq k'[[t]]$ and $k((t)) \otimes_k k' \simeq k'((t))$, $(\sum_i a_i t^i) \otimes \lambda \mapsto \sum_i \lambda a_i t^i$, are isomorphisms since k'/k is finite.)

By [Oe, Chapter V.8, Proposition], for a unipotent algebraic group U over a field k , U is k -wound if and only if $U(k[[T]]) = U(k((T)))$. The assertion then follows from this fact.

(4) First, assume that G' is k' -split, we will show that G is k -split by induction on $\dim G'$. If $\dim G' = 1$, i.e., $G' \simeq_{k'} \mathbb{G}_a$, then G is k -isomorphic to $\mathcal{R}_{k'/k} \mathbb{G}_a = \mathbb{G}_a^{[k':k]}$, which is k -split.

If $\dim G' > 1$ then there is a k -subgroup H' of G' such that H' is k' -split and the quotient $G/H' \simeq_{k'} \mathbb{G}_a$. The exact sequence of k' -groups

$$1 \rightarrow H' \rightarrow G' \rightarrow \mathbb{G}_a \rightarrow 1$$

induces the following exact sequence of k -groups ([Oe, Appendix 3, A.3.8])

$$1 \rightarrow \mathcal{R}_{k'/k} H' \rightarrow \mathcal{R}_{k'/k} G' = G \rightarrow \mathcal{R}_{k'/k} \mathbb{G}_a = \mathbb{G}_a^{[k':k]} \rightarrow 1.$$

From this exact sequence, we deduce that G is k -split.

Second, assume that G' is not k' -split we need to show that G is not k -split. In fact, if G' is not connected then by (2) G is not connected and hence G is not k -split. We may assume that G' is connected. Let G'_s be the k' -split of G' . Then $G'_w := G'/G'_s$ is k' -wound of dimension ≥ 1 . We have the following exact sequence of k' -groups

$$1 \rightarrow G'_s \rightarrow G' \rightarrow G'_w \rightarrow 1.$$

This exact sequence induces the following exact sequence of k -groups ([Oe, Appendix 3, A.3.8])

$$1 \rightarrow \mathcal{R}_{k'/k} G'_s \rightarrow G = \mathcal{R}_{k'/k} G' \rightarrow \mathcal{R}_{k'/k} G'_w \rightarrow 1.$$

As $\mathcal{R}_{k'/k} G'_w$ is k -wound by (3) and of dimension $= [k' : k] \dim G \geq 1$, it implies that G is not k -split. \square

6.3. Special versus split unipotent algebraic groups.

Definition 6.3. Let k be a field, G a smooth unipotent algebraic k -group. We define the following two properties

$$P(G; k) \quad H^1(k, G) = 0 \text{ if and only if } G \text{ is } k\text{-split.}$$

and

$$SP(G; k) \quad G \text{ is special if and only if } G \text{ is } k\text{-split.}$$

Remarks 6.4. (1) The property $\mathcal{P}(G/k)$ does not always hold in general, i.e., there is a field k and a smooth unipotent algebraic k -group G such that $H^1(k, G) = 0$ but G is not k -split.

(2) For any smooth algebraic unipotent k -group G , $P(G/k)$ implies evidently $SP(G/k)$.

Proposition 6.1 can be restated as the following corollary.

Corollary 6.5. *Let k be a field of characteristic $p > 0$, v a non-trivial valuation of k . We assume that k has a finite k^p -valuation basis. Let G a non-trivial smooth connected unipotent algebraic k -group of dimension $< p^m - 1$. Then the property $P(G; k)$ holds. \square*

Lemma 6.6. *Let k, K, L be fields such that L/k is a (not necessarily algebraic) separable extension, L/K is a finite extension. Let G be a smooth unipotent algebraic k -group. Denote by H the Weil restriction $\mathcal{R}_{L/K}(G \times_k L)$. Then if $P(H; K)$ holds then $SP(G; k)$ holds.*

Proof. Assume that G is special, in particular, $H^1(L, G) = 0$, we need to show that G is k -split. By Lemma 6.2 (1), $H^1(K, H) = H^1(L, G) = 0$. Hence as $P(H; K)$ holds, H is K -split. Also by Lemma 6.2 (4), G is L -split. Since L/k is a separable extension, G is also k -split by [Oe, Chapter V.7, Proposition]. \square

6.4. Proof of Theorem 1.2. If k_0 is perfect then k is perfect and G is always k -split and the assertion of the theorem holds trivially.

From now on, we assume that k_0 is not perfect. In particular, it implies that the characteristic of k_0 is $p > 0$. Note also that the valuation v on k_0 is non-trivial since otherwise by Lemma 5.9, $[k_0 : k_0^p] = 1$, i.e., k_0 is perfect, a contradiction.

If G is k -split then it is evident that G is special.

Assume now that G is special, in particular connected. We take a natural number m such that

$$[k : k_0] \cdot \dim G < [k_0 : k_0^p] p^m - 1,$$

and choose m variables y_1, \dots, y_m over k . We set

$$L := k(y_1, \dots, y_m) \text{ and } K := k_0(y_1, \dots, y_m).$$

Then L/k is a separable extension and L/K is a finite extension. Denote by H the Weil restriction $\mathcal{R}_{L/K}(G \times_k L)$. By Lemma 6.2, H is a connected unipotent K -group with

$$\dim H = [L : K] \dim(G \times_k L) \leq [k : k_0] \dim G < [k_0 : k_0^p] p^m - 1 = [K : K^p] - 1,$$

by the choice of m . (The last equality follows from [Bou1, Chapter V, 16.6, Corollary 3].) Therefore, Proposition 6.1 implies that $P(H; K)$ holds. Hence by Lemma 6.6, G is k -split. \square

6.5. Extension of valuations.

Lemma 6.7. *Let k be a field of characteristic $p > 0$ with a valuation v , Γ its value group. Let $K = k(x_1, \dots, x_r)$ be the field of rational functions in r variables x_1, \dots, x_r with coefficients in k . Then there is a unique valuation w on K with value group $\Gamma \times \mathbb{Z} \times \dots \times \mathbb{Z}$, r times, (with lexicographical order from the right) such that $w(a) = (v(a), 0, \dots, 0)$ for any $a \in k$ and $w(x_i) = (0, \dots, 1, \dots, 0)$, where 1 is at the $i + 1$ -th position.*

Furthermore, if k has a finite k^p -valuation basis with respect to v then K has a finite K^p -valuation basis with respect to w .

Proof. For the first assertion, see [Bou2, Chapter VI, Section 10.3, Theorem 1].

For the second assertion, by using induction on r , it suffices to consider the case $r = 1$.

Let $n = [k : k^p]$ and let $(b_i)_i, 1 \leq i \leq n$ be a valuation basis with respect to v of k^p -vector space k . Then we show that $(b_i x^j), 1 \leq i \leq n, 0 \leq j \leq p - 1$, is a valuation basis with respect to w of $k^p(x^p)$ -vector space $k(x)$.

Assume that $w(b_i x^j) \equiv w(b_k x^l)$ modulo p , or equivalently $(v(b_i), j) \equiv (v(b_k), l)$ modulo p . Hence $j \equiv l$ modulo p and $v(b_i) \equiv v(b_k)$ modulo p . This implies that $j = l$ and $i = k$. Therefore $(b_i x^j), 1 \leq i \leq n, 0 \leq j \leq p - 1$, are $k^p(x^p)$ -valuation independent with respect to w .

It can be checked that $[k(x) : k^p(x^p)] = [k : k^p] \cdot p = np$. Hence $(b_i x^j), 1 \leq i \leq n, 0 \leq j \leq p - 1$, is a $k^p(x^p)$ -valuation basis of k with respect to w . \square

Lemma 6.8. *Let k be a field of characteristic $p > 0$ with a valuation v , Γ its value group. Let $K = k((x_1, \dots, x_r))$ be the fraction field of the ring of formal power series in r variables x_1, \dots, x_r with coefficients in k . Then there is a valuation w on K with value group $\Gamma \times \mathbb{Z} \times \dots \times \mathbb{Z}$, r times, (with lexicographical order from the right) such that $w(a) = (v(a), 0, \dots, 0)$ for any $a \in k$ and $w(x_i) = (0, \dots, 1, \dots, 0)$, where 1 is at the $i + 1$ -th position.*

Furthermore, if k has a finite k^p -valuation basis with respect to v then K has a finite K^p -valuation basis with respect to w .

Proof. For simplicity of notation, we write a monomial $x_1^{n_1} \dots x_r^{n_r}$ as x^n , interpreting x as the vector (x_1, \dots, x_r) and n as (n_1, \dots, n_r) .

We define the map $w : k[[x_1, \dots, x_r]] \rightarrow \Gamma \times \mathbb{Z}^r$ as follows. Define $w(0) = \infty$, and for each element $0 \neq \sum_n a_n x^n \in k[[x_1, \dots, x_r]]$, choose the smallest index n_0 such that $a_{n_0} \neq 0$, and define

$$w\left(\sum_n a_n x^n\right) := (v(a_{n_0}), n_0).$$

Then w is a valuation on $k[[x_1, \dots, x_r]]$, i.e., w satisfies

- (1) $w(a + b) \geq \min\{w(a), w(b)\}$ for all $a, b \in k[[x_1, \dots, x_r]]$,
- (2) $w(ab) = w(a) + w(b)$ for all $a, b \in k[[x_1, \dots, x_r]]$,
- (3) $w(0) = 1$ and $w(0) = \infty$.

In fact, write $a = \sum_{n \geq n_0} a_n x^n$ with $a_{n_0} \neq 0$ and $b = \sum_{m \geq m_0} b_m x^m$ with $b_{m_0} \neq 0$, then we have

$$w(ab) = w\left(\sum_{n \geq n_0, m \geq m_0} a_n b_m x^{n+m}\right) = (v(a_{n_0} b_{m_0}), n+m) = (a_{n_0}, n) + (b_{m_0}, m) = w(a) + w(b).$$

For (2), without the loss of generality we may assume that $n_0 \leq m_0$ then $(v(a_{n_0}), n_0) \leq (v(b_{m_0}), m_0)$. If $n_0 < m_0$ then

$$v(a+b) = (v(a_{n_0}), n_0) = \min\{w(a), w(b)\}.$$

If $n_0 = m_0$ then $v(a_{n_0}) \leq v(b_{n_0})$ and

$$v(a+b) = (v(a_{n_0} + b_{n_0}), n_0) \geq (v(a_{n_0}), n_0) = \min\{w(a), w(b)\}.$$

Condition (3) is trivial.

By [Bou2, Chapter VI, Section 10, Proposition 4], we can extend uniquely w to a valuation $w : K = k((x_1, \dots, x_n)) \rightarrow \Gamma \times \mathbb{Z}^r$.

For the last assertion, let $s = [k : k^p]$ and b_1, \dots, b_s is a k^p -valuation basis of k then one can check that the values $v(b_i x_1^{n_1} \cdots x_r^{n_r})$, $1 \leq i \leq s$, $0 \leq n_1, \dots, n_r \leq p-1$ are pairwise distinct modulo p . In particular, these elements $b_i x_1^{n_1} \cdots x_r^{n_r}$ are k^p -linearly independent. This implies that $[K : K^p] \geq sp^r$.

On the other hand, $K = k((x_1, \dots, x_r))$ is the completion of $L = k(x_1, \dots, x_r)$ with respect to the valuation w' corresponding to (x_1, \dots, x_r) (note that in general w' is different from w constructed as above). Then one has

$$sp^r = [L : L^p] \geq [K : K^p],$$

the first equality follows from [Bou1, Chapter V, 16.6, Corollary 3] and the second inequality follows from [GO, Lemma 2.1.2]. Therefore, $[K : K^p] = sp^r$ and the elements $b_i x_1^{n_1} \cdots x_r^{n_r}$, $1 \leq i \leq s$, $0 \leq n_1, \dots, n_r \leq p-1$, form a K^p -valuation basis of K . \square

6.6. Geometric fields and Corollary 1.3. Lemma 6.7 and Lemma 6.8 motivate the following definition.

Definition 6.9. Let $k \subset K$ be two fields. We say that K is *geometric* over k if there is a tower of finite length of field extensions

$$K = K_0 \supset K_1 \supset K_2 \supset \cdots \supset K_n = k$$

such that $K_0 \supset K_1$ is a finite field extension and for each $i \geq 1$, we have

- (1) $K_i = K_{i+1}(x_1, \dots, x_r)$ for some variables x_1, \dots, x_r or
- (2) $K_i = K_{i+1}((y_1, \dots, y_r))$ for some variables y_1, \dots, y_r .

Corollary 6.10. *Let K be a field which is geometric over a perfect field k . Let G be a non-trivial smooth unipotent algebraic K -group. Then $\text{ed}_K(G) = 0$ if and only if G is K -split.*

Proof. By assumption there is a tower of finite length of field extensions

$$K = K_0 \supset K_1 \supset K_2 \supset \cdots \supset K_n = k$$

as in Definition 6.9. If $K_1 = K_n = k$ then K is perfect. The corollary then holds trivially.

Now assume that $K_1 \neq K_n$. On $K_n = k$ we consider the trivial valuation w_n . Then since K_n is perfect, K_n has a finite K_n^p -valuation basis with respect to w_n , namely $\{1\}$. Therefore by Lemma 6.7 and Lemma 6.8, the valuation w_n extend to a *non-trivial* valuation v on K_0 so that K_0 has a finite K_0^p -valuation basis with respect to v . The corollary now follows from Theorem 1.2. \square

Corollary 1.3 is just a very special case of Corollary 6.10.

6.7. Unipotent algebraic groups of dimension one. Over fields which are geometric over a perfect field, we can compute the essential dimension of smooth unipotent algebraic group of dimension 1 as follow.

Proposition 6.11. *Let k be a field which is geometric over a perfect field. Let G be a smooth connected unipotent algebraic k -group of dimension 1. Then $\mathrm{ed}_k(G) = 0$ if G is k -isomorphic to \mathbb{G}_a and $\mathrm{ed}_k(G) = 1$ otherwise.*

Proof. If $G \simeq_k \mathbb{G}_a$ then it is trivial that $\mathrm{ed}_k(G) = 0$.

Assume now that G is not k -isomorphic to \mathbb{G}_a , i.e., G is not k -split. In particular, it implies that k is not perfect and hence infinite. It is well-known that G is commutative and annihilated by p (G is in fact a k -form of \mathbb{G}_a). Therefore, by Lemma 4.5, $\mathrm{ed}_k(G) \leq 1$.

On the other hand, by Corollary 6.10, $\mathrm{ed}_k(G) \leq 1$ since G is not k -split. Therefore, $\mathrm{ed}_k(G) = 1$. \square

REFERENCES

- [BF] G. Berhuy and G. Favi, *Essential dimension: A functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003) 279-330.
- [Bo] A. Borel, *Linear Algebraic Groups (2nd ed.)*, Graduate texts in mathematics **126**, New York: Springer-Verlag 1991.
- [BLR] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 21. Springer-Verlag, Berlin, 1990.
- [Bou1] N. Bourbaki, *Elements of Mathematics: Algebra II, Chapters 4-7*, (translated by P. M. Cohn and J. Howie), Springer-Verlag 1990.
- [Bou2] N. Bourbaki, *Éléments de Mathématiques: Algèbre commutative, Chapitres 5 à 7*. Springer-Verlag Berlin Heidelberg 2006.
- [BR] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159-179.
- [BRV1] P. Brosnan, Z. Reichstein and A. Vistoli, *Essential dimension and algebraic stacks*, arXiv:math/0701903.
- [BRV2] P. Brosnan, Z. Reichstein and A. Vistoli, *Essential dimension of moduli of curves and other algebraic stacks*, (with an appendix by N. Fakhruddin), arXiv:0907.0924, to appear in Journal of European Mathematical Society.
- [CGP] B. Conrad, O. Gabber and G. Prasad, *Pseudo-reductive groups*, Series: New Mathematical Monographs (No. 17) (to appear).

- [DK] L. van den Dries and F. Kuhlmann, *Images of additive polynomials in $\mathbb{F}_q((t))$ have the optimal approximation property*, Canad. Math. Bull. **45** (2002), no. 1, 71-79.
- [Fl] M. Florence, *On the essential dimension of cyclic p -groups*, Invent. Math. **171** (2007), 175-189.
- [GO] O. Gabber and F. Orgogozo, *Sur la p -dimension des corps*, Invent. Math. **174** (2008), 47-80.
- [GM] P. Gille and L. Moret-Bailly, *Actions algébriques de groupes arithmétiques*, appendice à l'article de Ullmo-Yafaev "Galois orbits and equidistribution of special subvarieties: towards the André-Oort conjecture", prépublication.
- [Gro] A. Grothendieck, *Torsion homologique et sections rationnelles*, Anneaux de Chow et Applications, Séminaire Claude Chevalley, 1958, exposé n. 5.
- [JLY] C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials: Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications **45**, Cambridge University Press, 2002.
- [KM] N. Karpenko, A. Merkurjev, *Essential dimension of finite p -groups*, Invent. Math. **172** (2008), 491-508.
- [Le] A. Ledet, *On the essential dimension of p -groups*, Galois Theory and Modular Forms, Dev. Math., vol. **11**, Kluwer Acad. Publ., 2004, pp. 159-172.
- [LMMR] R. Lötscher, A. Meyer, M. MacDonald, Z. Reichstein, *Essential p -dimension of algebraic tori*, preprint 2009.
- [Me] A. Merkurjev, *Essential dimension*. Quadratic forms - algebra, arithmetic, and geometry, 299-325, Contemp. Math., **493**, Amer. Math. Soc., Providence, RI, 2009.
- [MZ] A. Meyer, Z. Reichstein, *Some consequences of the Karpenko-Merkurjev theorem*, to appear in the issue of Documenta Math. dedicated to Andrei Suslin's 60th birthday.
- [Oe] J. Oesterlé, *Nombre de Tamagawa et groupes unipotents en caractéristique p* , Invent. Math. **78** (1984), 13-88.
- [Re] Z. Reichstein, *Essential dimension*, to appear in Proceedings of the International Congress of Mathematicians 2010.
- [Se1] J.-P. Serre, *Espaces fibrés algébriques*, Anneaux de Chow et Applications, Séminaire Claude Chevalley, 1958, exposé n. 1.
- [Se2] J.-P. Serre, *Galois cohomology*, Corr. 2 printing; Springer 2002 (Springer Monographs in Mathematics).
- [TT1] Nguyen Q. Thang and Nguyen D. Tan, *On the Galois and flat cohomology of unipotent algebraic groups over local and global function fields. I*, J. Algebra **319** (2008), no. 10, 4288-4324.
- [TT2] Nguyen D. Tan and Nguyen Q. Thang, *Galois cohomology of unipotent algebraic groups and field extensions*, preprint (to appear in Comm. Algebra).
- [TV] D. Tossici and A. Vistoli, *On the essential dimension of infinitesimal group schemes*, arXiv:1001.3988 (to appear in Amer. J. Math.).

UNIVERSITÄT DUISBURG-ESSEN, FB6, MATHEMATIK, 45117 ESSEN, GERMANY AND INSTITUTE OF MATHEMATICS, 18 HOANG QUOC VIET, 10307, HANOI - VIETNAM

E-mail address: duy-tan.nguyen@uni-due.de